Dialogic

White Paper

Deploying Dialogic® ControlSwitch™ System Solution in the Amazon Web Service Public Cloud

Executive Summary

Traditional and next generation service providers are looking to public cloud infrastructure options to enhance service delivery agility and accelerate time-to-market. In order to do this, network functions need to operate efficiently within virtualized environments. A cloud native architecture that allows efficient scaling of functionality when and where applications require is important as service providers move infrastructure off purpose-built platforms and into public and private cloud environments.

The Dialogic® ControlSwitch™ System softswitch and the BorderNet™ Session Border Controller (SBC) can be deployed as a collection of Virtualized Network Functions (VNFs) in public cloud environments like the Amazon Web Services (AWS) to provide a feature-rich, carrier grade session and call control solution for delivering VoIP services.

Table of Contents

Introduction 4

Solution Description 4

The ControlSwitch Platform (CSP) 5

The Role of the Virtualized Session Border Controller 5

Service Flows into and Out of the Cloud 6

Deployment Considerations 6

AWS Network Layout 7

Summary 8

Deploying Dialogic® ControlSwitch™ System Solution in the Amazon Web Service Public Cloud

White Paper

Introduction

Moving network functionality to a cloud environment can improve flexibility and improve cost by allowing operators the ability to scale at software speeds where and when customer demand dictates. In addition, for large scale networks, being able to deploy the right amount of capacity at locations around the globe can help optimize performance on latency sensitive real-time applications. There is also the added benefit of not stranding physical assets compared to the traditional approach of deploying dedicated hardware at multiple locations around the globe.

The Dialogic ControlSwitch System provides cloud native capabilities with its unique modular architecture that decomposes functionality into discrete building blocks. With this approach, the underlying cloud computing infrastructure is used only when it is needed; for example, when processing a call request, the ControlSwitch System would draw the necessary resources on-demand (like compute servers or storage), perform a specific job, then relinquish the resources after the job was done. This implies that in production operation, the solutions could elastically scale resources based on traffic load and service demand.

This white paper describes the specific use case of deploying Dialogic's virtualized call and session control components in the Amazon AWS public cloud using Amazon Elastic Computing Cloud (EC2) resources and associated instantiation tools. A public cloud such as AWS has the benefit of a worldwide footprint of data centers along with on-demand IP connectivity whenever and wherever it is needed.

Solution Description

The ControlSwitch System and BorderNet SBC components can be deployed as Virtualized Network Functions (VNFs) within public and private cloud environments. The combined solution is aligned with ETSI Network Functions Virtualization (NFV) principals. It consists of VNF building blocks that together can be used to deploy a very scalable, feature-rich carrier grade VoIP network. The components of the Dialogic solution consist of the following software-based elements:

- **CSP** – ControlSwitch System Platform
- **EMS** – Element Management System
- **SBC** – BorderNet Session Border Controller
- **CDR** – Call Data Record element collector
- **AP** – Analytic platform

The solution components are instantiated within an Amazon VPC (Virtual Private Cloud) using Amazon EC2 API and tools and set up to provide Session Initiation Protocol (SIP) interfaces towards a service provider customer's Application Servers (AS) , access servers, as well as other fixed and mobile networks of other peering network operators. The Amazon EC2 tools provide the ability to efficiently scale up and scale down the solution components as needed.

The elements that make up the virtualized infrastructure to deliver a voice service are illustrated in Figure 1. In this scenario the functional modules that make up the call control platform and SBC are deployed in virtual machines in a self-contained VPC. It connects to another VPC where various virtualized application, Local Number Portability (LNP), authentication, routing and access gateway network functions are deployed in support of the customer's overall VoIP service. The media and signaling traverse the two VPCs through separate interfaces. The Dialogic solution includes the required interfaces on the ControlSwitch System to communicate with the applicable customer's servers to support the various call flows.

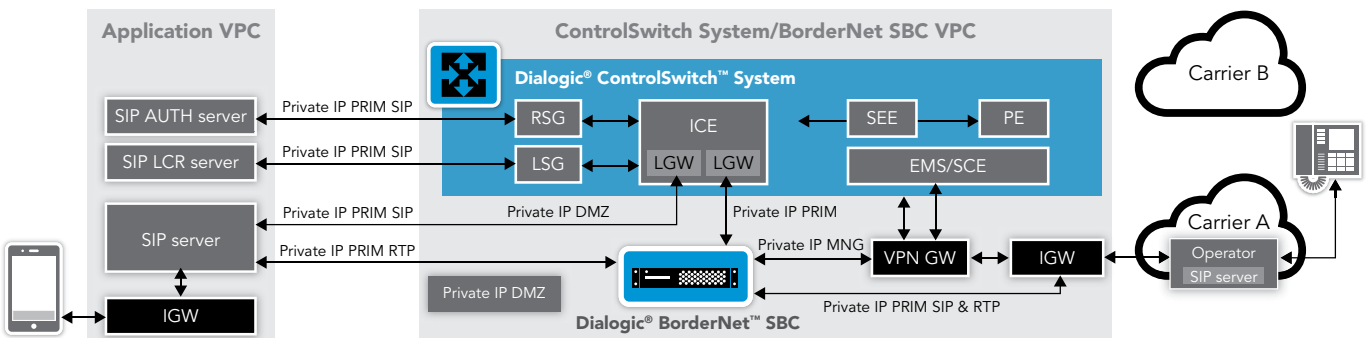

Figure 1 – VoIP service infrastructure using two Amazon VPCs

The Dialogic solution deployed in a VPC environment can accomodate high capacity carrier class services. Implementations such as this can be set up with the appropriate resources to support over 900 Call Attempts Per Second (CAPS). In addition to scalable performance in virtualized environments, the cloud-centric architecture and software defined networking between ConstrolSwitch System and BorderNet SBC VNFs as well as other VPCs involved in the end-to-end service enables increased service velocity and can result in reduced implementation time frames.

The ControlSwitch Platform (CSP)

Figure 1 details the ControlSwitch System components used to deliver a SIP protocol-based service. The ControlSwitch Platform (CSP) is collection of decomposed modules that support VoIP session control and routing policy related functions. The CSP is the infrastructure layer for these functions and provides efficient sharing of library files used across the various modules.

There are many VoIP session control functions supported by the CSP which can be used to create an extensive array of feature-rich High Definition VoIP services. The CSP also supports the various Point in Call (PIC) processing states for the Basic Call State Model such as user authorization for the service and querying an external Least Cost Routing (LCR) server.

The functions[1] supported by the CSP include the following:

- **ICE** – The IP Call Element is the SIP call control entity that manages and controls SIP trunk groups.
- **SEE** – The Service Execution Element handles the processing of individual sessions including handling the various PIC points for the lifetime of each call.
- **PE** – The Policy Engine entity provides the call handling intelligence for the Service Execution Element. On a per call basis, the SEE is first queries the PE for the call handling scheme and acts accordingly. In this use case, the scheme makes the SEE query external servers for service authorization and LCR.
- **LSG\RSG** – This entity provides Local Number Portability SIP Gateway and Routing SIP Gateway services for querying external severs. In this deployment scenario, a SIP 302 response is used to carry the relevant ported number information or routing information from the applciable server back to the CSP.
- **EMS** – The Element Management System is the primary platform for operating, creating, and configuring services. The EMS contains all the functionality to natively perform these workflows. It includes an integrated database so external platforms are not required for service creation, execution, and management.

In carrier grade applications, the CSP will also include the Call Data Record (CDR) platform. The CDR platform provides mediation services that include the programmable and on-demand collection and processing of CDRs. CDRs can be collected for post-processing without changing the existing production environment allowing the operator to build a self-contained system. The CDR platform performance can be varied based on an operator's needs; and changing the CSP instance type, increasing storage, or adding CDR instances do not impact service continuity.

The unique design of the CSP provides the ability to instantiate the various functional modules as needed. Scaling the service is made easier and VNF lifecycle management can be performed by adding or terminating the number of functional instances at the CSP level.

The Role of the Virtualized Session Border Controller

The BorderNet SBC is an all-software platform that supports multiple session control functions including routing, protocol mediation and manipulation, and transcoding. It serves as the front end to the public network, and also provides security features between the customer's network and the various end points in other connected service provider networks.

SIP header manipulation with the BorderNet SBC is highly flexible and makes the task of modification and normalization of tags, headers, and SDP parameters of SIP messages that traverse the network boundary easier. The BorderNet SBC's SIP-Profiler feature operates on dialog transactions and sessions to increase security, protect mission critical infrastructure, and enable service continuity and delivery. The customer is required to define specifically the SIP trunk parameters and features otherwise traffic will be blocked.

[1] *The Dialogic ControlSwitch System manual has a more detailed description of the CSP functions. Contact your account representative to find out more.*

The BorderNet SBC provides efficient processing and I/O of media traffic and supports software-based transcoding of an extensive list of traditional and next generation CODECs. In addition, SRTP support for the media streams provides an additional layer of security for the voice conversations.

Service Flows into and Out of the Cloud

The following service flows detail how calls are handled coming into the network from another operator to a subscriber (Ingress), and how calls are handled when originated by a subscriber going to a called party on another network (Egress).

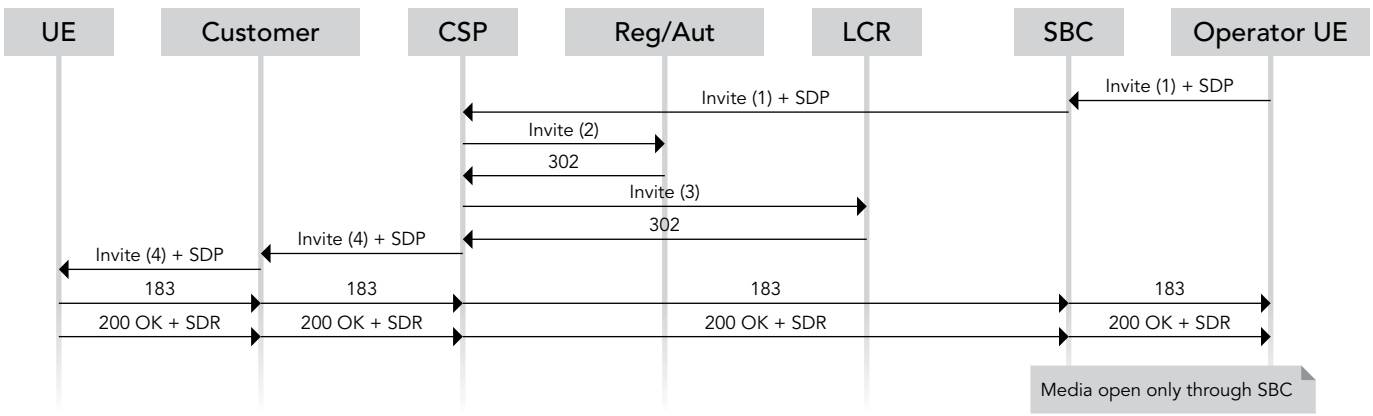

Figure 2 – AWS Dialogic's ControlSwitch ingress flow

On Ingress calls, authentication and routing to the customer's device is handled in the Application VPC. You'll also note that for both Ingress and Egress calls, the media streams are solely handled by the BorderNet SBC.

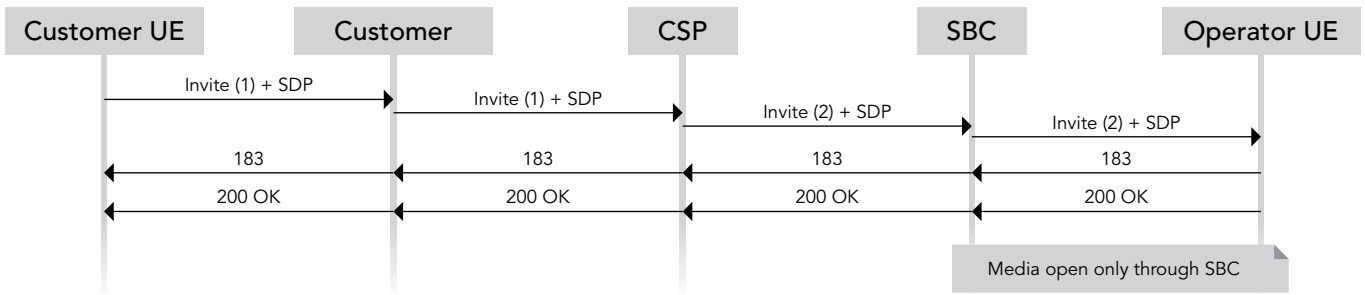

Figure 3 – AWS Dialogic's ControlSwitch Egress flow

Deployment Considerations

In an AWS implementation the user has the ability to deploy their applications within specific Availability Zones (AZ). Each AWS data center is considered a region. Within each data center region there are multiple AZs. AZs are set up to provide isolation for applications running within them from failures in other AZs. In addition, AZs within a region are connected to each other by inexpensive, low latency links. One way of protecting from failure in a single location is by instantiating VNFs in separate AZs. Regions and AZs can be selected through the tools provided by AWS.

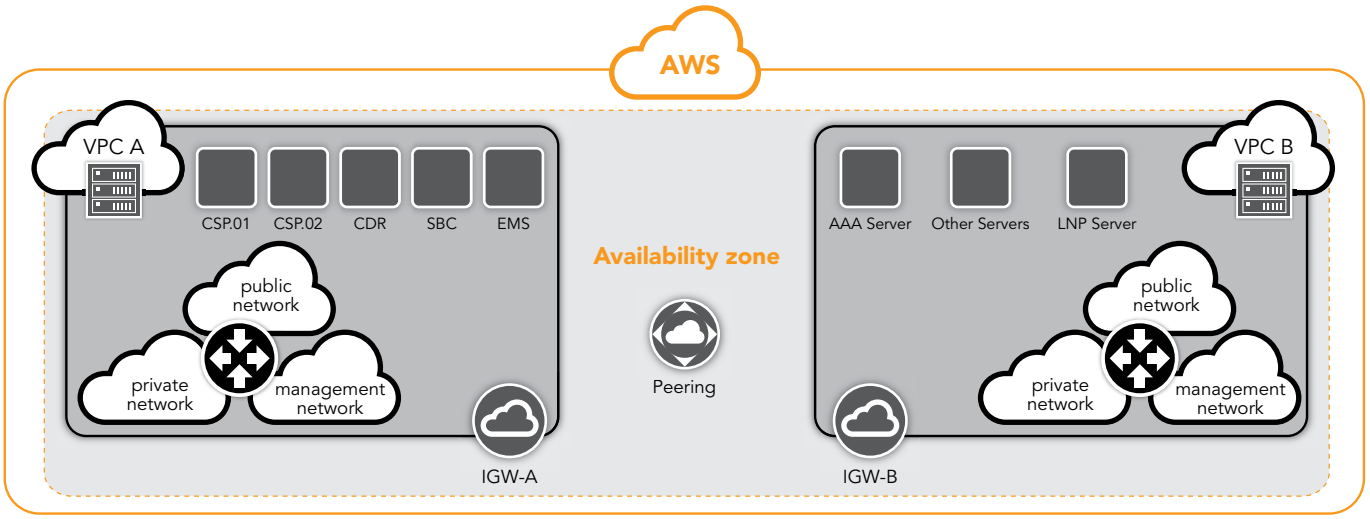

Figure 4 – Amazon AWS service deployment

In this scenario, the two VPCs are deployed in one Availability Zone. Additional instances of the Dialogic VNFs would be required if more AZs were added.

The AWS VPC network is isolated and is based on the provided AWS router. The route tables provide the required routing schemes for traffic within and between the VPCs as well as for traffic destined for the Internet. The scenario here assumes an AWS VPC containing the ControlSwitch System and BorderNet SBC is connected over the appropriate subnets to another AWS VPC that contains the customer's own server instances. However, that may not always be the case. This design is not limited to a scenario where a customer's entire infrastructure is contained within adjacent AWS VPCs or even in different Availability Zones. The customer may be using a combination of public and private clouds to deploy its infrastructure, and may also include Physical Network Functions (PNFs) to support the service. For such a case, the Dialogic solution can be deployed in the public cloud and the reachability to other customer's servers would be via the public Internet.

The ControlSwitch System solution for public cloud environments requires a VPN gateway (GW) at the edge of the VPC. The VPN GW creates the secured VPN for the Dialogic VNFs as well as the configuration and management of the solution.

In this deployment scenario, one EIP (Elastic IP) is sufficient. It is used for public connection of SIP trunk groups to other service providers. The same EIP may be also be used also for secured VPN dial in. However, we recommend the use of a dedicated EIP for VPN dial in for better security.

One of the other benefits a customer gains by deploying the ControlSwitch System solution in the public cloud is access to worldwide efficient networking and connectivity. Major public cloud providers like Amazon, provide ubiquitous, high quality connectivity everywhere. For international carriers deploying the ControlSwitch System solution in AWS, international links can be obtained as part of the public cloud services.

AWS Network Layout

The example deployment discussed in this use case is based on deploying the following required subnets:

- **Management Subnet (Mng. SubNet)** – This subnet is used to connect the management peers of the solution components. For each element, the management interface is the VNF management interface. Specifically, the management interface also provides web-based access to the CSP vEMS and the SBC for network management tasks.
- **Private Subnet (Priv. SubNet)** – This subnet is used for internal traffic between the Dialogic solution elements as well as with the customer's servers in the Application VPC. Amazon EC2 tools provide a PEERING feature that facilitates making connections between the VPCs.
- **Public Subnet (Pub. SubNet)** – This subnet is used for connecting end user traffic and traffic to other carriers via the public Internet. Amazon EC2 tools are used for associating the Elastic IP (EIP) Address to **Pub. SubNet** interface. In this use case, the SBC interfaces this subnet and is associated with specific EIP. This EIP (or another dedicated one) is being used for the **Mng. SubNet** connection. A VPN-GW provides the ability for remote users to enter the **Mng. SubNet**.

Summary

Public cloud environments can give both traditional and next generation service providers a cost effective method to deploy infrastructure in a scalable manner without having to deploy dedicated servers. Cloud native applications that are modular in design are important in achieving the benefits that virtualization and ultimately full NFV will provide. The combination of cloud native capabilities, world class ControlSwitch System features, and improved analytics gives service providers the ability to take advantage of Cloud/NFV benefits and deliver advanced VoIP services to customers at accelerated rates.

Dialogic continues to invest in developing carrier grade solutions to help service providers move functionality to the cloud and bridge the technology gap between legacy voice and VoIP networks. Dialogic's deployment of call routing and session control VNFs in the Amazon AWS cloud is an example of how service providers can take advantage of advances in virtualization, server and cloud management technologies to increase flexibility and reduce costs and improve the rate at which services are delivered.

www.dialogic.com

For a list of Dialogic locations and offices, please visit: https://www.dialogic.com/contact.aspx

11/16 14718-01